



UNITED STATES PATENT AND TRADEMARK OFFICE

un
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,799	01/15/2004	Hemant Kumar Jain	INT-102/US	8270

30869 7590 03/16/2007
LUMEN INTELLECTUAL PROPERTY SERVICES, INC.
2345 YALE STREET, 2ND FLOOR
PALO ALTO, CA 94306

EXAMINER

SHAIFER HARRIMAN, DANT B

ART UNIT	PAPER NUMBER
----------	--------------

2109

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/759,799	JAIN, HEMANT KUMAR	
	Examiner	Art Unit	
	Dant B. Shaifer - Harriman	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| <p>1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)</p> <p>2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)</p> <p>3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date <u>5/28/2004</u>.</p> | <p>4) <input type="checkbox"/> Interview Summary (PTO-413)
 Paper No(s)/Mail Date. ____.</p> <p>5) <input type="checkbox"/> Notice of Informal Patent Application</p> <p>6) <input type="checkbox"/> Other: ____.</p> |
|---|---|

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: the "Control and Statistics Block" as indicated in the specification is labeled "308" when it should be labeled "314" as indicated in the Figure 3.

Appropriate correction is required.

2. The disclosure is objected to because of the following informalities: in paragraph 0094, "Multicast Meter 604" should be "Multicast Flood Meter 604," as indicated in Figure 6 of the specification.

Appropriate correction is required.

3. The disclosure is objected to because of the following informalities: in paragraph 0094, "Multicast Flood Meter 603" should be "Multicast Flood Meter 604," as indicated in Figure 6.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Art Unit: 2109

4. Claims 8 -10 & 18- 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim #8, #9, #18, #19, #20 are vague and indefinite, because one would not know whether a "network characteristic" is referring to a particular type of intrusion flood packet or statistical analysis of the data rate flow over a period of time in the normal operating limits of the apparatus. Furthermore, one would also not know if there is a difference between a "network characteristic" and a "particular network characteristic," of the apparatus.

Claims 1-9 & 12-20 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Each limitation of claims above regard an apparatus, which is a machine. The limitations in the claims above further limit the scope of the limitations to software, which clearly aren't machine parts. It is unclear to the examiner that instead machine parts the limitations are directed towards software, this is the basis for the rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-10 & 11- 20 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*. Each limitation of the above claims is drawn towards software *per se*, which is clearly non-statutory subject matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims(s) 1-5, 7-20 are rejected under 35 U.S.C. 102(b) as being taught by Malan et al. (US PG PUB # 2002/0032871)

Malan teaches:

Claim #1 & #11: An apparatus capable detecting and preventing plurality of rate based and non rate based denial service attacks, said apparatus comprising:
host having a threshold estimation mechanism

Art Unit: 2109

estimating traffic thresholds based on past traffic, baseline,

trend, and seasonality (Paragraph: 0040); and

an intrusion prevention apparatus operatively coupled to

said host, said intrusion prevention apparatus comprising:

an intrusion prevention logic, and computer executable instructions controlling

said intrusion prevention logic (Paragraph: 0040)

a media access controller (MAC) interface (Paragraph: 0062, Figure # 4);

a classification means operatively coupled to said MAC

interface for classifying data packets received from said MAC

interface according to Layer 2, Layer 3, and Layer 4

classifications, said classification means being capable of

enforcing Layer 2, Layer 3, Layer 4 accepted header

syntax(Paragraph: 0064, Figure #4);

a meter means operatively coupled said classification

means, said meter means having a plurality of meters and being

capable maintaining statistics of said attacks and

determining whether a threshold has been reached(Paragraphs: 0068, Figure #

5);

a decision multiplexer means operatively coupled to said

meter means, said decision multiplexer means being capable of

accepting decisions from said plurality of meters and informing a single decision

to said MAC interface(Paragraph: 0067, Figure #5); and

an ager means capable of timing flood states

identified by said classification means or by said meter means, said ager means comprising continuous learning mechanism for continuously learning and updating said statistics(Paragraphs: 0068, Figure # 5).

Claim #2 & #12: The apparatus of claim1, wherein said plurality of meters detect and prevent rate based denial of service attacks selected from the group consisting of: synchronization (SYN)flood), Transmission Control Protocol (TCP) flood, Internet Control and Message Protocol (ICMP) flood, User Datagram Protocol (UDP) flood, port scan, source flood, destination flood, broadcast flood, Address Resolution Protocol (ARP) flood, Reverse ARP (RARP) flood, multicast flood, Virtual Local Area Network (VLAN) flood, double encapsulated VLAN flood, protocol flood, Internet Protocol (IP) option flood, fragment flood, port flood, Layer floods, Layer floods, and Layer 4 floods (Paragraph: 0080 & 0081, Figure #7, the examiner notes that claims 2 and 12 are duplicates and that claim 12 is the implementation of claim 2 on a computer readable medium, which when implement produces the same result.

Claim # 3 & #13: The apparatus of claim 2, wherein said rate based denials of service attacks are to an end node or from said end node to other nodes on the internet (Paragraphs: 0062, Figures: 4 & 6 & 7, the examiner notes that claims 3

Art Unit: 2109

and 13 are duplicates and that claim 13 is the implementation of claim 3 on a computer readable medium, which when implement produces the same result.

Claim #4 & #14: The apparatus of claim 1, further comprising:

a SYN flood detection and prevention mechanism having a support means creating plurality legitimate IP addresses during normal operation when the TCP state transitions to ESTABLISHED (Paragraph 0030, the examiner further notes that claims 4 and 14 are duplicates and that claim 14 is the implementation of claim 4 on a computer readable medium, which when implement produces the same result.

Claim # 5 & #15: The apparatus claim 4, wherein said SYN flood detection and prevention mechanism allows only said plurality of legitimate IP addresses to be stored during normal operation (Paragraph 0030, the examiner further notes that claims 5 and 15 are duplicates and that claim 15 is the implementation of claim 5 on a computer readable medium, which when implement produces the same result.

Claim #7 & #17: The apparatus claim 1, further comprising: a source tracking mechanism multiplicatively incrementing count for sources that send identified flood data, thereby distinguishing said sources from others that send non-flood data (Paragraphs: 0077 & 0078, the examiner further notes that claims 7 and 17 are duplicates and that claims 17 is the implementation of claim 7 on a computer

Art Unit: 2109

readable medium, which when implement produces the same result.

Claim # 8 & #18 the apparatus of claim 1, wherein said ager means collects continuous learning data for different network characteristics (Paragraphs: 0068, examiner notes: that the storm profiler of the collector inherently continuously collects statistical data or network characteristics and updates the storm detector which keeps a database on the various data packet anomalies.

The examiner further notes that claims 8 and 18 are duplicates and that claims 18 is the implementation of claim 8 on a computer readable medium, which when implement produces the same result. (The examiner note that it is inherent that the alert message generated by the collector (i.e. the storm detector) is sent to the zone controller who then blocks those particular data packet anomalies entering the system.

Claim # 9 the apparatus of claim 8, wherein said plurality of meters identify whether a threshold of counts for a particular network characteristic has been reached (Paragraphs: 0068, the examiner notes: that the storm profiler which is an integral part of the collector constantly obtains statistical data on packet flow characteristics, when any particular predetermined threshold is over flowed with that particular data packet and an anomaly alert message is generated and sent to the local controller, then the message is sent

Art Unit: 2109

to the zone controller for a mass distribution of the anomaly alert message to the rest of the apparatus.

Claim # 10: The apparatus of claim 9, wherein said threshold has been reached and said plurality of meters inform said decision multiplexer means to block traffic with said particular network characteristic for a certain time period. (Paragraph 0084, the examiner notes that it is inherent that the collector-storm detector collects statistical information on other data packet anomalies besides SYN-packet anomalies and whether or not they have reached the predetermined threshold. The examiner also notes that after a data packet anomaly has been detected, and an alert message has been sent to the rest of the system, it is inherent that the apparatus will block that particular data packet flow that contains those particular data packet anomalies.

Claim #19: The system of claim 18, wherein said threshold estimation mechanism further comprises: a means for producing traffic forecast for said network characteristics; and a means for determining said traffic thresholds and a deviation of said traffic forecast. (Paragraph 0065 & 0066 & 0067 & 0068, the examiner further notes that among the various statistical information being studied by the collector, the collector must have some idea of what normal data packet traffic flow in order to know when various data packet anomalies occur, it is inherent that data packet traffic forecast, threshold, and deviation of traffic forecast is also studied.

Claim #20: The system of claim 18, wherein said particular network characteristic is destination port (Paragraph: 0035).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim # 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US PG PUB # 2002/0032871 A1) in view of Malan et al. (US PG PUB # 2002/0035698 A1).

Malan (#2002/0032871 A1) discloses the features of claimed invention as discussed above.

Malan (#2002/0032871 A1) fails to teach a zombie flood detection and prevention mechanism having a means for limiting connections said plurality of legitimate IP addresses stored during normal operation; and a means for determining threshold for said connections based on baseline traffic learned during normal operation.

However Malan (# 2002/0035698 A1) does teach a flood detection and prevention mechanism that limits or attenuates connections of said plurality of legitimate IP address (Paragraph: 0066)

Malan (#2002/0032871 A1) and Malan (# 2002/0035698 A1) are analogous art because they are from the Blocking of Denial of Service attacks field.

At the time of invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Malan (#2002/0032871 A1) and Malan (# 2002/0035698 A1) before him or her, to modify the storm detector of Malan (#2002/0032871 A1, Paragraph 0068), to include specifically a zombie flood detection and prevention mechanism of Malan (# 2002/0035698 A1) because the storm detector is enabled to record and analyze data packet anomalies, the modification will allow the storm detector to detect and prevent zombie floods, which are limiting the connections that use legitimate IP addresses that are stored during normal operation of configuration.

The suggestion/motivation for doing so would have been to increase the storm detector capabilities such that it detects SYN – Floods, other types of floods, and Zombie Floods, that establish connections with legitimate IP addresses, that aren't normally characterized as a virus by the usual definition of what a typical virus characteristic, thereby increasing its efficiency (Malan et al. (US PG PUB # 2002/0035698 A1, 0062).


Art Unit: 2109

Therefore, it would have been obvious to combine Malan (# 2002/0035698 A1) with Malan (#2002/0032871 A1) to obtain the invention as specified in the instant claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dant B. Shaifer - Harriman whose telephone number is 571-272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


JOSEPH DEL SOLE
SUPERVISORY PATENT EXAMINER
3/15/07